T2147-906761-US3845/PB

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Valerie FAVIER ET AL.

Serial No.: 09/740,801

Filed: December 21, 2000

For: METHOD AND DEVICE FOR CONFIGURING A FIREWALL IN A COMPUTER SYSTEM

Examiner:

Group Art Unit:

Corres. To FR 99/16118
Filed December 21, 1999

McLean, Virginia

SUPPLEMENTAL PRELIMINARY AMENDMENT

Honorable Commissioner of Patents and Trademarks
Washington, DC 20231

Sir:

Prior to examination of the above-identified application, please amend the application as follows:

IN THE SPECIFICATION:

Page 1, after the title and before the first paragraph, insert the following heading at the left-hand margin:

--Field of the Invention--;

Page 1, line 8, delete "The Prior Art" and substitute –Description of Related Art— at the left-hand margin;

Page 4, line 1, delete "Presentation of the Figures" and substitute the following heading at the left-hand margin:

--Brief Description of the Drawings--;

Page 4, at line 15, delete "Description of an Embodiment of the Invention" and substitute the following heading at the left-hand margin:

--Detailed Description of the Preferred Embodiment(s)--;

Page 11, after the last paragraph ending "...global.", insert the following new paragraph:

--While this invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the preferred embodiments of the invention as set forth herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention as set forth herein and defined in the claims—

IN THE CLAIMS:

Please cancel claims 1 – 10 in their entirety and without prejudice and substitute the following new claims:

--11. A method for configuring a firewall (1) in a computer system (2) comprising objects (3), and resources (4), for establishing an access control policy for the objects (3), the method comprising grouping the objects (3) of the system into internal and external protection domains (5, 6), ensuring establishing a firewall (a) for protection of an internal domain (5) relative to an external domain (6), and applying to the firewall a rule for controlling access between a source resource (4) and a destination resource only if said source and destination resources belong to the same internal or external protection domain (5 or 6).

12. A method according to claim 11, further comprising determining the protection domain of the resources (4) by means of firewall network interfaces (10) through which communications pass in order to reach said resources.

13. A method according to claim 12, further comprising defining zones (8) comprising networks or subnetworks, associating the network interfaces (10) of firewalls to which said zones are connected with an internal or external domain, determining the incoming and outgoing network interfaces (10) of current traffic, analyzing whether said network interfaces are attached to an internal or external domain, and applying the rule for controlling access only if both network interfaces are attached to the same internal domain (5), and the resources belong to the same protection domain.

14. A method according to claim 11, characterized in that it composes groups of objects (3) for which the access control policy is identical and the rule for controlling access is applied between each of the resources of a source group and a destination group.

15. A method according to claim 12, characterized in that it composes groups of objects (3) for which the access control policy is identical and the rule for controlling access is applied between each of the resources of a source group and a destination group.

16. A method according to claim 13, characterized in that it composes groups of objects (3) for which the access control policy is identical and the rule for controlling access is applied between each of the resources of a source group and a destination group.

17. A method according to claim 11, further comprising characterizing the rule for controlling access with a local or global scope, applying the rule to the resources in question only if said resources belong to the same protection domain (5) or (6) when the scope of the rule is local, and applying the rule to all of the resources in question when the scope of the rule is global.

18. A method according to claim 12, further comprising characterizing the rule for controlling access with a local or global scope, applying the rule to the resources in question only if said resources belong to the same protection domain (5) or (6) when the scope of the rule is local, and applying the rule to all of the resources in question when the scope of the rule is global.

19. A method according to claim 13, further comprising characterizing the rule for controlling access with a local or global scope, applying the rule to the resources in question only if said resources belong to the same protection domain (5) or (6) when the scope of the rule is local, and applying the rule to all of the resources in question when the scope of the rule is global.

20. A method according to claim 14, further comprising characterizing the rule for controlling access with a local or global scope, applying the rule to the resources in question only if said resources belong to the same protection domain (5) or (6) when the scope of the rule is local, and applying the rule to all of the resources in question when the scope of the rule is global.

21. A method according to claim 15, further comprising characterizing the rule for controlling access with a local or global scope, applying the rule to the resources in question only if said resources belong to the same protection domain

(5) or (6) when the scope of the rule is local, and applying the rule to all of the resources in question when the scope of the rule is global.

22. A method according to claim 16, further comprising characterizing the rule for controlling access with a local or global scope, applying the rule to the resources in question only if said resources belong to the same protection domain (5) or (6) when the scope of the rule is local, and applying the rule to all of the resources in question when the scope of the rule is global.

23. A device for configuring a firewall (1) in a computer system (2) comprising resources (4) including objects (3) having an access control policy and an established central configuration machine (14) for grouping the objects (3) of the system into internal (5) and external (6) protection domains, a firewall (1) ensuring the protection of an internal domain (5) relative to an external domain (6), and means for applying to the firewall in question a rule for controlling access between a source resource (4) and a destination resource only if said source and destination resources belong to the same protection domain (5) or (6).

24. A device according to claim 23, characterized in that it further comprises a graphical interface (15) from which an administrator (7) can enter the domains (5) and (6) and the access control rules.

25. A device according to claim 23, characterized in that the graphical interface allows the administrator (7) to define a local or global scope for the access control rule, and in that the machine (14) applies the rule to the resources in question only if said resources belong to the same protection domain (5) or (6) when the scope of the rule is local, and applies the rule to all of the resources in question when the scope of the rule is global.

26. A device according to claim 24, characterized in that the graphical interface allows the administrator (7) to define a local or global scope for the access control rule, and in that the machine (14) applies the rule to the resources in question only if said resources belong to the same protection domain (5) or (6) when the

scope of the rule is local, and applies the rule to all of the resources in question when the scope of the rule is global.--

IN THE ABSTRACT:

Please add the following Abstract.

REMARKS

This Supplemental Preliminary Amendment is made to eliminate informalities in the specification, claims and abstract resulting from a literal translation of the French text, to eliminate the use of multiple dependent claims, and to insert headings to conform the application to U.S. practice.

The present application is believed to be in condition for examination, which action is earnestly solicited.

Respectfully submitted,

Miles & Stockbridge P.C.

Date 3/13/01

By: _____
Edward J. Kondracki
Registration No. 20,604

Miles & Stockbridge, P.C.
1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
Tel.: (703) 903-9000